Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for detecting fraud in one of a credit card or debit card system, the system generating network event records, each network event record being generated in response to an event in the system, the method comprising:

~~determining whether the system is a credit card system or a debit card system;~~

performing at least [[one]] a first fraud detection test and a second different fraud detection test on the network event records ~~based on the determination of whether the system is a credit card system or a debit card system~~;

generating a first fraud alarm upon detection of suspected fraud by ~~the at least one~~ the first fraud detection test;

generating a second different fraud alarm upon detection of suspected fraud by the second different fraud detection test;

correlating the generated first fraud ~~alarms~~ alarm with the generated second different fraud alarm based on common aspects of the ~~fraud alarms,~~ first fraud alarm and the second different fraud alarm, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and

responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case.

2. (previously presented) The method of claim 1, wherein the method is performed by computer executable instructions disposed on at least one computer readable medium.

3. (previously presented) The method of claim 2, wherein the computer executable instructions are distributed among a plurality of hardware platforms.

4. (canceled).

5. (previously presented) The method of claim 2, wherein at least a portion of the computer executable instructions are implemented in a core infrastructure.

6. (currently amended) The method of claim 1, wherein the ~~at least one~~ first fraud detection test or the second different fraud detection test includes ~~the step of~~ normalizing the network event records such that the network event records conform to a predetermined format.

7. (currently amended) The method of claim 1, wherein the ~~at least one~~ first fraud detection test or the second different fraud detection test includes ~~the step of~~ enhancing the network event records such that an enhanced network event records include data obtained from at least one external system.

8. (previously presented) The method of claim 7, wherein the enhanced network event record includes data obtained from at least one database.

9. (previously presented) The method of claim 8, wherein the at least one database includes at least one of a configuration database, an event database, a billing database, a history database, and/or a records database.

10. (currently amended) The method of claim 1, wherein the ~~at least one~~ first fraud detection test or the second different fraud detection test includes a comparison of at least a portion of the network event records to a threshold rule, the first fraud alarm or second different fraud alarm being generated if one network event record violates the threshold rule.

11. (currently amended) The method of claim 10, wherein the first fraud alarm or second different fraud alarm is generated if a value in one network event record exceeds a threshold value specified by the threshold rule.

12. (currently amended) The method of claim 10, wherein the first fraud alarm or second different fraud alarm is generated if a value in one network event record does not equal a value specified by the threshold rule.

13. (currently amended) The method of claim 1, wherein the ~~at least one~~ first fraud detection test or the second different fraud detection test includes a comparison of at least a portion of the network event records to a profile detection rule, the first fraud alarm or second different fraud alarm being generated if one network event record violates the profile detection rule.

14. (previously presented) The method of claim 13, wherein the one network event record is compared to a normal usage profile.

15. (previously presented) The method of claim 13, wherein the one network event record is compared to a fraudulent usage profile.

16. (previously presented) The method of claim 13, wherein the profile detection rule is based on historical network event records.

17. (currently amended) The method of claim 1, wherein the ~~at least one~~ first fraud detection test or the second different fraud detection test includes a comparison of at least a portion of the network event records to a predetermined pattern to identify a normal usage and/or a fraudulent usage.

18. (previously presented) The method of claim 17, wherein the predetermined pattern is based on history data.

19. (previously presented) The method of claim 17, wherein the predetermined pattern is generated by a neural network.

20. (previously presented) The method of claim 17, wherein the comparison is performed using tree-based algorithms that generate discrete output values.

21. (previously presented) The method of claim 17, wherein the comparison is performed using statistical based algorithms that that employ iterative numerical processing techniques.

22. (currently amended) The method of claim 1, wherein the ~~step of~~ correlating includes ~~the step of~~ enhancing a network event record by obtaining relevant data from an external source.

23. (currently amended) The method of claim 1, wherein the ~~step of~~ correlating includes ~~the step of~~ applying at least one predetermined fraud analysis rule to the network event records to decide if a fraud case is appropriate.

24. (currently amended) The method of claim 1, wherein the ~~step of~~ correlating includes ~~the step of~~ applying at least one predetermined prioritization rule to the fraud case to obtain the priority of the fraud case.

25. (previously presented) The method of claim 1, wherein the fraud prevention action may be performed automatically, semi-automatically, or manually based on the priority.

26. (previously presented) The method of claim 1, wherein the fraud prevention action is selected from a group that is comprised of at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification.

27. (currently amended) The method of claim 1, wherein the first fraud alarm or second different fraud alarm is selected from a group that is comprised of at least one of a pin hacking alarm or a geographic alarm.

28. (canceled)

29. (currently amended) The system of claim [[28,]] 67, wherein the ~~fraud~~ detection ~~system~~ element is dynamically reconfigured to adjust fraud detection rules in accordance with changing patterns of fraud.

30. (canceled).

31. (currently amended) The system of claim [[30,]] 67, wherein the priority is based on a severity of suspected fraud.

32. (currently amended) The system of claim [[30,]] 67, wherein the detection element includes at least one software processing engine comprising computer executable instructions disposed on at least one computer readable medium.

33. (previously presented) The system of claim 32, wherein the at least one software processing engine is distributed among a plurality of hardware platforms.

34. (canceled).

35. (previously presented) The system of claim 32, wherein the at least one software processing engine includes a rules based thresholding engine configured to read the network event record and compare data in the network event record to a predetermined threshold.

36. (previously presented) The system of claim 35, wherein the rules based thresholding engine further comprises:

at least one rules database;

a normalizer configured to configure the network event record into a standardized format;

an enhancer component coupled to the normalizer, the enhancer component being configured to insert additional data in the network event record; and

a threshold detector coupled to the enhancer component, the threshold detector being configured to compare a network event record to at least one threshold rule obtained from the at least one rules database, whereby the alarm is generated if the network event record violates the at least one threshold rule.

37. (previously presented) The system of claim 36, wherein the enhancer component is coupled to an external systems interface, the additional data including data received from an external system.

38. (previously presented) The system of claim 36, wherein the network event record includes an event key and at least one feature, the event key identifying the network event and the at least one feature including event measurement data.

39. (previously presented) The system of claim 38, wherein the measurement data includes a count of a number of occurrences of an event during a predetermined time period.

40. (previously presented) The system of claim 38, wherein the measurement data includes a count of a number of like events occurring simultaneously.

41. (previously presented) The system of claim 38, wherein the measurement data includes geographic velocity data.

42. (currently amended) The system of claim 36, wherein the at least one rules database comprises:

an enhancement rules database coupled to the enhancer component, the enhancer component obtaining an enhancement rule from the enhancement rules database based on data in the network event record; and

a threshold detection rules database coupled to the threshold detector, the threshold detector obtaining a threshold rule in accordance with data in the network event record.

43. (previously presented) The system of claim 42, wherein the enhancement rule directs the enhancer component to select external data from a selected external source.

44. (previously presented) The system of claim 42, wherein the threshold rule stipulates that an alarm is generated when data in the network event record exceeds a threshold value.

45. (previously presented) The system of claim 42, wherein the threshold rule stipulates that an alarm is generated when data in the network event record does not equal a threshold value.

46. (currently amended) The system of claim 36, wherein the enhancer component provides the threshold detector with a feature vector, the feature vector including [[the]] an event key and a plurality of feature event values, the event key including suspected fraud event identifying data, each feature event value of the plurality of feature event values providing fraud event measurement data.

47. (previously presented) The system of claim 46, wherein the feature event value includes a threshold value.

48. (previously presented) The system of claim 46, wherein the feature vector includes a name field, a value field, and a generating event field for each feature.

49. (previously presented) The system of claim 48, wherein the feature vector is implemented as a data structure, the data structure being stored on a computer readable medium.

50. (previously presented) The system of claim 48, wherein the feature vector includes at least one contributing event field for each feature.

51. (currently amended) The system of claim 32, wherein the at least one software processing engine in the detection element further comprises:

a profiling database including at least one profile detection rule; and

a profiling engine configured to compare the network event record with at least one profile in accordance with the at least one profile detection rule, the profiling engine generating

the first fraud alarm or second different fraud alarm if the network event record substantially violates the profile detection rule.

52. (previously presented) The system of claim 51, wherein the profile includes a normal use profile and/or a fraudulent use profile.

53. (previously presented) The system of claim 51, wherein the profile is based on historical network event records.

54. (previously presented) The system of claim 32, wherein the at least one software processing engine in the detection element comprises a pattern recognition engine configured to identify normal and/or fraudulent patterns of usage.

55. (previously presented) The system of claim 54, wherein the pattern recognition engine compares the network event record to history data obtained from a history database.

56. (previously presented) The system of claim 54, wherein the pattern recognition engine includes a neural network configured to identify fraudulent patterns of usage.

57. (previously presented) The system of claim 54, wherein the pattern recognition engine includes tree-based algorithms.

58. (currently amended) The system of claim 54, wherein the pattern recognition engine includes statistical based algorithms that [[that]] employ iterative numerical processing techniques.

59. (currently amended) The system of claim [[30,]] 67, wherein the analysis element further comprises:

an external systems interface component configured to obtain data from external systems relevant to the first fraud alarm or the second different fraud alarm; ~~alarms;~~

a configuration database configured to specify [[any]] additional data ~~required~~ for fraud alarm analysis;

an alarm enhancement component coupled to the external systems interface and the configuration database, the alarm enhancement component being configured to add the additional data and external system data to the first fraud alarm or the second different fraud alarm; and

a fraud case builder component coupled to the alarm enhancement component, the fraud case builder being configured to correlate and consolidate fraud alarms.

60. (previously presented) The system of claim 59, wherein the fraud case builder is coupled to a rules database, the rules database providing the fraud case builder with parameters for generating fraud cases.

61. (currently amended) The system of claim [[30,]] 67, wherein the expert element further comprises:

a configuration database configured to specify [[any]] additional data ~~required~~ for alarm analysis based on an alarm configuration;

an external systems interface component configured to obtain data from external systems relevant to at least one of the first fraud alarm or second different fraud alarm; ~~alarms;~~ and

a prioritizer component coupled to the configuration database and the external systems interface, the prioritizer component being configured to direct the external system interface to obtain the additional data from at least one external system based on configuration data obtained from the configuration database, the prioritizer adding the additional data to the fraud case.

62. (previously presented) The system of claim 61, wherein the prioritizer component receives prioritization rules from the configuration database and prioritizes the fraud case ~~cases~~ in accordance with the prioritization rules.

63. (previously presented) The system of claim 62, wherein the prioritization rules specify the fraud prevention action.

64. (currently amended) The system of claim 63, further comprising an enforcement component coupled to the prioritizer component, the enforcement component performing the fraud prevention action based on the ~~enhanced~~ priority of the fraud case.

65. (currently amended) The system of claim [[30,]] 67, wherein the fraud prevention action includes at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification.

66. (currently amended) The system of claim [[30,]] 67, wherein the first fraud alarm or second different fraud alarm includes at least one of a pin hacking alarm or a geographic alarm.

67. (new) A system for monitoring one or more of a plurality of credit card or debit card networks, each network being configured to generate network event records, each network event record being generated in response to an event occurring in the network, the system comprising:

a detection element configured to generate a first fraud alarm if a network event record is in violation of a first fraud detection rule, the detection element generating a second different fraud alarm if a network event record is in violation of a second different fraud detection rule, the first fraud alarm and the second different fraud alarm having at least one common aspect;

an analysis element configured to correlate the first fraud alarm and the second different fraud alarm, and generate a fraud case based on the correlated fraud alarms; and

an expert element configured to assign a priority to the generated fraud case, and to perform a fraud prevention action in accordance with the priority.